

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

FILED
ASHEVILLE, NC
JUL 18 2019U.S. DISTRICT COURT
W. DISTRICT OF N.C.

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Electronic items listed in Attachment A currently in HSI
Charlotte, NC custody located at 3700 Arco Corporate
Drive, Suite 300, Charlotte, NC 28273

Case No.

3:19 mj 237

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Western District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

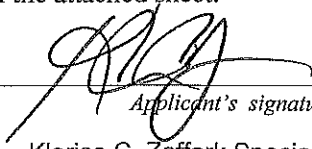
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(2)	Distribution/Receipt of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2422(b)	Coercion and Enticement

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature


Klarisa C. Zaffark Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date:

7/18/2019


Judge's signature

City and state: Asheville, North Carolina

W. Carleton Metcalf, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

FILED
ASHEVILLE, NC
JUL 18 2019
U.S. DISTRICT COURT
W. DISTRICT OF N.C.

IN THE MATTER OF THE §
SEARCH OF THE FOLLOWING: §
ELECTRONIC ITEMS LISTED IN §
ATTACHMENT A THAT ARE HELD AT THE §
HSI CHARLOTTE OFFICE §
LOCATED AT 3700 ARCO CORPORATE DRIVE §
SUITE 300, CHARLOTTE, NC 28273 §

CASE NO. 3:19 mj 237

I, Klarisa C. Zaffark, being duly sworn, depose and state the following:

1. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI). I have been so employed from May 2010, to the present. I am currently assigned to HSI Hendersonville, North Carolina office. As part of my official duties, I have conducted and participated in investigations relating to narcotics smuggling, human smuggling and trafficking, document fraud, and the sexual exploitation of children. I have also received training and instruction in the field of investigating child pornography. As part of my duties and responsibilities as an HSI Special Agent, I am authorized to investigate crimes involving the sexual exploitation of children pursuant to Title 18, United States Code, Section 2251, et seq.
2. As a result of my training and experience, I am familiar with methods employed by individuals engaged in various illegal activities, including the coercion and enticement of minors, travel with intent to engage in illicit sexual conduct, and interstate transportation of child pornography. I am aware, as a result of my training and experience, that child pornography is not generally available in retail establishments, even from those which offer other explicit sexual material. Persons who wish to obtain child pornography do so by ordering and/or obtaining it by discreet contact with other individuals and underground businesses that have child pornography collections. I am further aware, based on my training and experience, that: individuals engaged in

the interstate transportation of child pornography often obtain the child pornography from electronic devices that have the capability of connecting to the Internet; individuals who obtain child pornography from the Internet often store the child pornography on additional electronic devices capable of storing digital media; likewise, individuals who coerce and/or entice minors often utilize such electronic devices such as cellular phones and computers to communicate with minors via the Internet; and, said individuals utilize such electronic devices when coordinating interstate travel to engage in illicit sexual conduct with minors. I am further aware, based on my training and experience, that: individuals utilize internet chat rooms and social media to meet and/or communicate with minors for the purpose of online solicitation, and that these individuals who meet minors through chat rooms and social media often divert their communications to email and text messages via electronic devices with email and texting capabilities, including such devices as a cellular phone.

3. This affidavit is submitted in support of an application for a search warrant for the following items: one (1) Samsung Galaxy S9 Model: SM-G960U (IMEI: 354823091053923), one (1) Samsung Galaxy S7 Model: SM-G930V (IMEI: 355301076129918), one (1) Samsung Tablet Model: SM-T580 (SN: R52K20RQ3XT), one (1) SanDisk 16GB USB (SN: BL131124774B), one (1) SanDisk 64GB USB (SN: BN130323461B), and five (5) PNY 8GB USB's. The aforementioned items are currently being held as evidence at the HSI Charlotte Office located at 3700 Arco Corporate Drive, Suite 300, Charlotte, North Carolina 28273. These items were seized from Todd Andrew RILEY.

4. Your Affiant is personally familiar with facts and circumstances surrounding this investigation, both from my own investigative activities, and from information obtained from other law enforcement officers/agencies.

5. As more fully described below, your Affiant has probable cause to believe that presently and/or at the time of this warrant's execution, evidence of child pornography, coercion and enticement of a minor and production of child pornography will be found inside the following items: one (1) Samsung Galaxy S9 Model: SM-G960U (IMEI: 354823091053923), one (1) Samsung Galaxy S7 Model: SM-G930V (IMEI: 355301076129918), one (1) Samsung Tablet Model: SM-T580 (SN: R52K20RQ3XT), one (1) SanDisk 16GB USB (SN: BL131124774B), one (1) SanDisk 64GB USB (SN: BN130323461B), and five (5) PNY 8GB USB's. I have reason to believe the above listed items will contain items which constitute evidence of the commission of the crime of certain activities including the receipt, possession, distribution, or transportation of child pornography in violation of Title 18, United States Code, § 2252A(a)(1), (a)(2), or (a)(5)(B) in addition to Title 18, United States Code, § 2422(b) and Title 18, United States Code, § 2251(a), 2251(e) relating to the sexual exploitation of minors.

6. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, § 2252A(a)(1), (a)(2), and (a)(5)(B), Title 18, United States Code, § 2422(b) and Title 18, United States Code, § 2251(a), 2251(e) is presently located in the above listed items.

RELEVANT STATUTES

7. This investigation concerns alleged violations of Title 18, United States Code, § 2252A(a)(1), (a)(2), and (a)(5)(B), Title 18, United States Code, § 2422(b) and Title 18, United States Code, § 2251(a), 2251(e) relating to the sexual exploitation of minors.

8. Title 18 U.S.C. § 2252A(a)(1) makes it a federal offense for any person to knowingly

transport or ship in interstate or foreign commerce by any means, including by computer, any visual depiction if such visual depiction involves the use of a minor engaging in sexually explicit conduct. Section 2252A(a)(2) makes it a federal crime for any person to knowingly receive or distribute child pornography that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means, including computer, or knowingly reproduce any visual depiction for distribution in interstate or foreign commerce by any means, including by computer, or through the mail. Section 2252A(a)(5)(B) makes it a federal crime for any person to knowingly possess, or access with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer.

9. Title 18, United States Code, § 2422(b) makes it a federal offense for any person using the mail or any facility and means of interstate or foreign commerce, who knowingly persuades, induces, entices and coerces any individual who has not attained the age of 18 years, to engage in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.

10. Title 18, United States Code, § 2251(a) makes it a federal offense for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of

such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed. Section 2251(e) makes it a federal crime for any individual to attempt or conspire to violate this section.

DEFINITIONS

11. The following definitions apply to this Affidavit:

12. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

13. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

14. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer

image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

15. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

16. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

17. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys

or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

18. “Domain Name” refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level or top-level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and “.edu” for educational organizations. Second level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

19. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

20. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

21. A “hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result

in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

22. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

23. An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

24. “Internet Service Providers” or “ISPs” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.

25. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
26. "Memory Card", a memory card or flash card is an electronic flash memory data storage device used for storing digital information. They are commonly used in many electronic devices, including digital cameras, mobile phones, laptop computers, MP3 players and video game consoles. They are small, re-recordable, and able to retain data without power.
27. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
28. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.
29. The terms "records", "documents", and "materials", as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs,

digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

30. “Remote computing service,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

31. “Smart Phone”, a Smart Phone is a mobile phone that utilizes a mobile operating system similar to the way a traditional computer uses an operating system to function. Smart Phones are typically capable of storing various types of media files, including image, video and audio files; of accessing the Internet through wireless or cellular data connections and Internet browsing software; of capturing still images and video through integrated cameras built into the device; of accessing electronic mail accounts; and providing services utilizing the Global Positioning System.

32. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

33. “Uniform Resource Locator” or “Universal Resource Locator” or “URL” is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific

computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

34. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

35. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND REGARDING SEIZURE OF COMPUTERS

36. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

37. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drives and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

38. Searching computer systems for criminal evidence is a highly technical process requiring expert skills in a properly controlled environment. The vast array of computer hardware and

software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

39. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

40. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

Child Pornography

41. Based upon my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the sexual exploitation of children which includes both the distribution, receipt, possession and collection of child pornography as well as individuals who try to persuade and entice minors to engage in illicit sexual conduct:

a. Individuals with a sexual interest in children receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals with a sexual interest in children collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower, or "groom," the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with a sexual interest in children almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home. Individuals with a sexual interest in children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. “Child erotica,” as used in this Affidavit, is defined as materials or items that are sexually arousing to certain individuals, but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

e. Likewise, Individuals with a sexual interest in children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the collector to view the collection, which is highly valued.

f. Individuals with a sexual interest in children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in sex with children or child pornography.

g. Individuals with a sexual interest in children prefer not to be without their child

pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND REGARDING THE INTERNET

42. I have been formally trained in the investigation of crimes involving the sexual exploitation. I also own my own computer and have personal knowledge of the operation of a computer. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

43. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider ("ISP") that connects to the Internet. The ISP assigns each user an Internet Protocol ("IP") Address. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

44. Photographs and other images can be used to create data that can be stored in a computer. This storage can be accomplished using a "scanner", which is an optical device that can recognize characters on paper and, by using specialized software, convert them to digital form. Storage can also be captured from single frames of video and converted to an image file. After the photograph or other image has been scanned into the computer, the computer can store the data from the image as an individual "file". Such a file is known as an image file. Computers are capable of displaying an image file as a facsimile of the original image on a computer screen.

45. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 1 terabyte (1,000 gigabytes) are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

46. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and or print out a hard copy of the image by using a printer device (such as a laserjet or

inkjet).

47. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

BACKGROUND ON KIK AND KIK REPORTS

48. Kik Messenger (hereinafter “Kik”) is a mobile application designed for chatting or messaging owned and operated by Kik Interactive, Inc. According to the publicly available

document “Kik’s Guide for Law Enforcement,”¹ to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

49. According to “Kik’s Guide for Law Enforcement,” Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

50. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik’s Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it

¹ Available at: <https://lawenforcement.kik.com/hc/en-us/categories/200320809-Guide-for-Law-Enforcement>.

independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images is critically important to protecting their users, product, brand, and business interests.

51. Kik is located in Ontario, Canada and is governed by Canadian law. According to information contained in the “Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary” (hereinafter Kik Glossary), which Kik provides when reporting information to law enforcement authorities, Kik is mandated to report to the Royal Canadian Mounted Police (RCMP) any images and/or videos that would constitute suspected child pornography under Canadian law which are discovered on the Kik platform. According to the Kik Glossary, Kik is typically alerted to suspected child pornography on Kik based on digital hash value matches to previously identified child pornography or through reports from other Kik users or third-party moderators.

52. The RCMP has advised Homeland Security Investigations (HSI) agents that upon receiving a report from Kik related to suspected child pornography, the RCMP reviews the reported IP addresses of the Kik users contained in the Kik Reports to determine their location. The RCMP then provides Kik Reports of Kik users in the United States to HSI in Ottawa, Canada, who in turn provides the Kik Reports to the HSI Cyber Crimes Center (C3) Child Exploitation Investigations Unit (CEIU) located in Fairfax, Virginia for analysis and dissemination.

BACKGROUND OF INVESTIGATION

53. Your affiant has reviewed a Kik Report dated December 26, 2018. A review of the Kik Report shows that on December 26, 2018, a Kik user utilizing username “Fox_man_courageous”

utilized the Kik application to upload an image of child pornography as described herein. The Kik Report detailed “Fox_man_courageous” provided the following subscriber information:

First Name: Todd

Last Name: Riley

Email: Toddriley77@gmail.com

Username: Fox_man_courageous

Phone Brand: Verizon

Type: Android

Model: SM-G930V

54. Your affiant has learned that Kik was alerted to the child pornography image on December 26, 2018 through the use of SafePhoto technology. According to the Kik Glossary, Kik has developed an internal hash matching system called “SafePhoto” (similar to Microsoft’s PhotoDNA system) that is used to scan images uploaded via Kik for suspected child pornography. Kik’s SafePhoto database is comprised of hash values obtained from the International Criminal Police Organization (hereinafter “INTERPOL”), the RCMP and the National Center for Missing and Exploited Children (hereinafter “NCMEC”). Kik uses SafePhoto to run a hash value check against every image sent within Kik, including within private conversations, in order to detect images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When a user sends an image with a hash value that matches a child exploitation hash value in the SafePhoto database, Kik removes the content from its communications system, closes the user’s account and provides a SafePhoto report of the incident to the RCMP.

55. According to Kik's SafePhoto report, the reported image was flagged based upon a hash value provided to Kik by NCMEC. According to information provided to HSI by NCMEC, the NCMEC hash set provided to Kik is comprised of images submitted to NCMEC by U.S. companies through its CyberTipline and contains hashes derived from images and videos that have been reviewed and agreed upon by two NCMEC personnel to: (1) depict either prepubescent children or pubescent children that have been identified by law enforcement; (2) engaging in sexual contact, which may involve the genitals, mouth or digits of a perpetrator or contact with a foreign object, or an animal involved in sexual behavior with a child, or a lewd or lascivious exhibition of the genitalia or anus of a child.

56. Along with Kik's Report, Kik provided the Secure Hash Algorithm Version 1 (hereinafter SHA1 hash value/s) [Z5JZQVQ2P3Y64P7Q2PHNYEG7BYEI7W4Z] for the suspected child pornography image that Kik reported to the RCMP. Your affiant knows from training and experience that a hash value is akin to a fingerprint for a digital file. In order to generate a hash value, the contents of a file are processed through a cryptographic algorithm, and a unique numerical value – the hash value – is produced that identifies the unique contents of the file. If the contents are modified in any way, the value of the hash will also change significantly.

57. On June 25, 2019, HSI personnel searched law enforcement databases for the SHA1 hash value [Z5JZQVQ2P3Y64P7Q2PHNYEG7BYEI7W4Z] provided by Kik and identified the exact same corresponding SHA 1 hash value [Z5JZQVQ2P3Y64P7Q2PHNYEG7BYEI7W4Z] in a law enforcement database. HSI personnel received information that the SHA1 hash value listed above was recognized to be a hash match to a file of an identified child/series but was unable to retrieve the image for review. HSI personnel did NOT open or view any images provided by Kik to the RCMP.

58. The information provided by Kik included IP addresses associated with access to the pertinent Kik user account. Specifically, IP address 24.246.142.65 was used by “Fox_man_courageous” on December 26, 2018 to distribute/upload a child pornography image. In addition, IP address 24.246.142.65 was used to access the Kik user account during the same month the Kik user distributed/upload the child pornography image.

59. A query of the American Registry for Internet Numbers (“ARIN”) online database revealed that IP address 24.246.142.64 used on December 26, 2018 to distribute/upload a child pornography image was registered to Morris Broadband. In addition, the IP address 24.246.142.64 used to access the Kik user account during the month the Kik user distributed/uploaded a child pornography image was also registered to Morris Broadband.

60. On June 24, 2019, an HSI Customs summons (ICE-HSI-SV-2019-00313) was issued to Morris Broadband requesting subscriber information for IP address 24.246.142.64. A review of the results obtained on June 26, 2019 identified the following account holder information:

Lease Start: 2018-12-10 21:49:30 ET

Lease Expiration: 2019-06-25 11:19:38 ET

Modem Mac: 14:CF:E2:1C:51:09

Device Mac: 2C:30:33:53:0F:FB

Billing Account: 006296

First Name: TODD

Last Name: RILEY

Physical Address: 137 SHORTY COLLINS ST EAST FLAT ROCK NC 28726-4013

Billing Address: Same as physical address

Telephone Number: (828) 697-7809; (828) 693-2000

Customer Since: 6/29/2005

61. A search of law enforcement databases that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for a Todd Riley (herein referred to as RILEY) residing in the Western North Carolina area. These records resulted in the following:

Name: Todd Andrew RILEY

D.O.B. 11/19/1977

Address: 137 SHORTY COLLINS ST EAST FLAT ROCK NC 28726

DL: NC-26313967

62. Additionally, database checks revealed RILEY was the registered owner of a 2009 Subaru Forester 2.5X bearing North Carolina license plate NC/AJB8904 registered to the address of 137 Shorty Collins St., East Flat Rock, NC 28726.

63. On June 25, 2019, HSI Hendersonville agents traveled to RILEY's residence located at 137 Shorty Collins St., East Flat Rock, North Carolina. Upon arrival to the residence, HSI agents knocked on the door and were greeted by RILEY's mother and father. Agents requested to speak with RILEY and were informed RILEY was at work located at the General Electric (GE) Lighting manufacturer located in East Flat Rock, North Carolina. RILEY's parents informed the agents that RILEY lived with them and occupied a room within the residence. RILEY's parents informed the agents that RILEY would not be returning home until late afternoon.

64. At approximately 1135 hours (EST), HSI agents traveled to RILEY's place of employment General Electric (GE) Lighting manufacturer located at 3010 Spartanburg Hwy, East Flat Rock, NC 28726. Upon arrival agents asked to speak with a Human Resource Officer and were informed she was out of the office but could be contacted via phone. A GE employee

contacted the Human Resource Officer via cellular phone and explained investigators wanted to speak with her. Special Agent (SA) Klarisa Zaffark communicated with the Human Resource Officer and explained that she was requesting RILEY be excused to speak with investigators. HSI Agents were escorted to a private conference room within the business and stated RILEY would be informed of the investigator's presence.

65. At approximately 1215 hours (EST), RILEY was escorted into the private conference room to meet with investigators. Upon entry, SA Zaffark introduced herself along with SA Farmer, Task Force Officer (TFO) Thiel and Computer Forensic Analyst (CFA) Olsen. SA Zaffark informed RILEY that she was working on an investigation involving child exploitation offenses and believed RILEY may have information useful to the investigation. SA Zaffark informed RILEY that he was not under arrest and that although they were in a private room within his employers building, RILEY was free to leave at any time and return to his duties. RILEY stated he understood and was willing to speak with investigators.

66. RILEY began by providing biographical information and stated he resides at 137 Shorty Collins St., East Flat Rock, NC 28726 with his parents since he attended high school. RILEY stated he has been employed at GE Manufacturing in East Flat Rock, NC for approximately twenty-three (23) years.

67. SA Zaffark asked RILEY if he had any idea as to why investigators would want to speak with him about a child exploitation investigation. RILEY stated he utilized the Kik Messenger application and may have been involved in private rooms within the application where child pornography was traded.

68. RILEY stated he downloaded the Kik Messenger application approximately four (4) to five (5) years ago. RILEY informed investigators his Kik username was "Fox_man_courageous"

and had not utilized the username for approximately three (3) years. RILEY explained to investigators that he utilized the application on his previous cellular device and no longer uses the Kik application on his current phone.

69. SA Zaffark asked RILEY if he had a cellular device with him in the room. RILEY stated he had his Samsung Galaxy S9 in his pocket and removed it for investigators to observe. SA Zaffark asked RILEY if he would be willing to consent to the search of his cellular device for evidence of child exploitation material. SA Zaffark explained HSI CFA Olsen would conduct a forensic preview on his device and return the device to him if no evidence of child pornography was discovered. RILEY provided SA Zaffark with a verbal consent. SA Zaffark provided RILEY with a Department of Homeland Security Consent to Search Form and filled in the description of the cellular device. RILEY provided investigators with the phone number of (828)-808-3732 as the phone number to the cellular device and stated no passcode was needed to review the phone. SA Zaffark read the consent to search form out loud to RILEY and asked if he understood and was able to read and write. RILEY responded "Yes" and voluntarily signed the DHS Consent to Search Form. The cellular device was provided to HSI CFA Olsen for a forensic preview and as result, CFA Olsen discovered multiple digital images of child pornography.

70. Immediately following the discovery, RILEY admitted to investigators that he had been involved in rooms where child pornography was being trade while utilizing the Kik application. RILEY stated he would on many occasions be in multiple rooms at the same time and if someone posted a link with child pornography that he liked, he would copy the link. RILEY explained he would then post the link containing the child pornography in another chat room to get a reaction out of other users.

71. RILEY stated he was first been exposed to a child pornography image in 2004 while

utilizing Yahoo chat rooms. RILEY stated he mainly observed adult pornography but was first exposed to a professional Russian LS-Model image². RILEY admitted to utilizing numerous live streaming³ applications to communicate with underage girls and have them send him nude images and videos of themselves engaging in sexual acts. RILEY stated many of the applications have the option to simultaneously chat with users while observing them live. RILEY explained he would observe an underage girl or a group of underage girls while utilizing a live stream application and instruct them to take their clothes off and engage in sexual acts on themselves. RILEY informed investigators that he utilized an independent recording application to record the minors as they engaged in the sexual acts while utilizing the VIBO live stream application. RILEY informed investigators he was mainly recording and in communication with girls around the age range of nine (9) to eleven (11) years of age.

72. RILEY informed investigators he believed he may have communicated with approximately one hundred (100) underage girls. RILEY admitted to utilizing the live streaming applications, VIBO Live, Telegram and LiveMe.

73. RILEY informed investigators the he utilized Telegram on the phone prior to purchasing his current Samsung Galaxy S9 and that the application can be used to trade bigger files like the Kik application. RILEY informed investigators that the old cellular device contained evidence of child pornography and was stored in his room at his residence.

74. RILEY informed investigators that he had a Samsung Galaxy Note Tablet and a few

² LS Studio/LS-Models images/videos are commonly observed in the online child exploitation community. LS Studio is known to law enforcement as a previously operated online subscription service and photography studio that created photographic images of young teens and prepubescent girls in sexually explicit poses.

³ Live streaming refers to online streaming media utilized to transmit and receive live video and audio coverage over the Internet. User interaction via chat rooms forms a major component of live streaming.

thumb drives at his residence that may contain evidence of child pornography.

75. SA Zaffark asked RILEY if he would be willing to return with investigators to his personal residence to retrieve all electronic devices that may contain evidence of child pornography. RILEY agreed and stated he understood what he was doing was wrong and no longer wanted to have the devices in his possession.

76. At approximately 1445 hours (EST), RILEY and HSI investigators departed from the GE Manufacturing building and walked towards the parking lot. RILEY provided investigators with consent to search for any weapons in RILEY's personal vehicle before allowing him to enter the vehicle and lead investigators back to his residence. TFO Thiel searched RILEY's vehicle and found the vehicle to contain no weapons.

77. Upon arrival to RILEY's residence, RILEY's father was observed outside on the front porch. SA Farmer approached RILEY's father and explained that RILEY was assisting with an investigation and asked if it would be ok if investigators entered the residence to retrieve some electronic devices from RILEY. RILEY's father provided investigators with consent to enter the residence. SA Zaffark and TFO Thiel entered the residence and communicated with RILEY's father in the dining room of the residence. SA Farmer and CFA Olsen were escorted by RILEY to his bedroom and began to provide investigators numerous electronic devices.

78. Once outside of the residence, SA Zaffark asked RILEY if he believed all the items he provided investigators contained evidence of child pornography, to which RILEY responded "Yes.". RILEY agreed to abandon all electronic devices provided to investigators and signed a DHS Notice of Abandonment Form abandoning the following items:

One (1) Galaxy S7 Cell Phone Model# SM-G930V (IMEI: 355301076129918)

One (1) Samsung Galaxy S9 Model# SM-G906 (IMEI: 354823091053923)

One (1) Samsung Tablet Model# SM-T580 / SN: R52K20RQ3XT

One (1) Gateway Computer Model# DX4850 / SN: PTGBL02017109005730100

One (1) SanDisk 16GB USB (SN: BL131124774B)

One (1) SanDisk 64GB USB (SN: BN130323461B)

Five (5) PNY 8GB USB drives

79. All items listed above and detailed within the signed DHS Notice of Abandonment Form (DHS Form 4607) were seized by HSI Agents and transported by CFA Olsen to the SAC Charlotte, North Carolina evidence vault located at 3700 Arco Corporate Drive, Suite 300, Charlotte, North Carolina 28273 pending a full forensic analysis.

CONCLUSION

80. Based on the foregoing facts, I respectfully submit that there is probable cause to believe that evidence of child pornography, coercion and enticement of minors and other evidence of the use of computers to produce and transport child pornography as set forth in the search warrant, will be found on the following:

one (1) Samsung Galaxy S9 Model: SM-G960U (IMEI: 354823091053923),

one (1) Samsung Galaxy S7 Model: SM-G930V (IMEI: 355301076129918),

one (1) Samsung Tablet Model: SM-T580 (SN: R52K20RQ3XT),

one (1) SanDisk 16GB USB (SN: BL131124774B),

one (1) SanDisk 64GB USB (SN: BN130323461B),

five (5) PNY 8GB USB drives.


81. I am aware that the recovery of data by a computer forensic analyst takes significant

time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from RILEY. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

82. Your Affiant respectfully requests that a warrant be issued authorizing HSI Special Agents, with appropriate assistance from other law enforcement personnel and/or agencies to seize and search the above referenced items.


Klarisa C. Zaffark
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 18th day of July 2019


W. Carleton Metcalf
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF NORTH CAROLINA

ATTACHMENT A

SUBJECT PROPERTY TO BE SEARCHED

Electronic Device currently in the secure custody of:

HSI CHARLOTTE OFFICE
LOCATED AT 3700 ARCO CORPORATE DRIVE
SUITE 300, CHARLOTTE, NC 28273

one (1) Samsung Galaxy S9 Model: SM-G960U (IMEI: 354823091053923)

one (1) Samsung Galaxy S7 Model: SM-G930V (IMEI: 355301076129918)

one (1) Samsung Tablet Model: SM-T580 (SN: R52K20RQ3XT)

one (1) SanDisk 16GB USB (SN: BL131124774B)

one (1) SanDisk 64GB USB (SN: BN130323461B)

five (5) PNY 8GB USB drives

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, § 2252A(a)(1), (a)(2), and (a)(5)(B), Title 18, United States Code, § 2422(b) and Title 18, United States Code, § 2251(a), 2251(e).

1. All electronic files containing child pornography and images of child pornography in any form, information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256 and records or other items which evidence ownership or use of computer that is currently saved on: one (1) Samsung Galaxy S9 Model: SM-G960U (IMEI: 354823091053923), one (1) Samsung Galaxy S7 Model: SM-G930V (IMEI: 355301076129918), Samsung Tablet Model: SM-T580 (SN: R52K20RQ3XT), one (1) SanDisk 16GB USB (SN: BL131124774B), one (1) SanDisk 64GB USB (SN: BN130323461B), five (5) PNY 8GB USB's
2. Records, documents, writings, and correspondences with others pertaining to the coercion, enticement, production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct.
3. Any and all, photographs, letters, written narratives and computer text files or electronic

matter to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct.

4. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the items described in Attachment A and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, or storage media.
5. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct.
6. Records or other items which evidence ownership or use of computer equipment listed in Attachment A, including, but not limited to, correspondence, sales receipts, and bills for Internet access relating any other Internet service provider, email addresses.
7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, letters, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote

computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of collection, advertising, transport, distribution, receipt, or possession of child pornography.
9. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.
10. For any computer hard drive or other electronic media (hereinafter, "MEDIA") that is called for by this warrant, or that might contain things otherwise called for by this warrant:
 - a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;
 - b. passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;
 - c. documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.
11. Visual depictions, in whatever form, including digital, of minors engaged in sexually explicit conduct.
12. Records or data in any form relating to the following:

- a. communications with other individuals engaged in the trading of child pornography
- b. records and information relating or pertaining to the identity of the person or persons using or associated with Kik username "Fox_man_courageous"